



成長可能性に関する説明資料

株式会社FFRI
(東証マザーズ・3692)



会社概要

会社概要

- 会社名： 株式会社 F F R I (FFRI, Inc.)
- 所在地： 東京都渋谷区恵比寿1-18-18 東急不動産恵比寿ビル4階
- 役員：

代表取締役社長	鵜飼 裕司
取締役最高技術責任者	金居 良治
取締役最高財務責任者	田中 重樹
取締役（非常勤）	高橋 郁夫
常勤監査役	近藤 正二
監査役（非常勤）	下吹越 一孝
監査役（非常勤）	杉山 由高
- 設立： 2007年7月3日
- 資本金： 1億2,580万円
- 事業内容：
 1. コンピュータセキュリティ研究、コンサルティング
 2. ネットワークシステムの研究、コンサルティング、情報提供、教育
 3. コンピュータソフトウェア及びコンピュータプログラムの企画、開発、販売、リース、保守、管理、運営及びこれらに関する著作権、出版権、特許権、実用新案権、商標権、意匠権等の財産権取得、譲渡、貸与及び管理
 4. 上記事業に関連する一切の業務



社名とコーポレートマークに込めた思い

FourteenForty Research Institute



コーポレートマーク

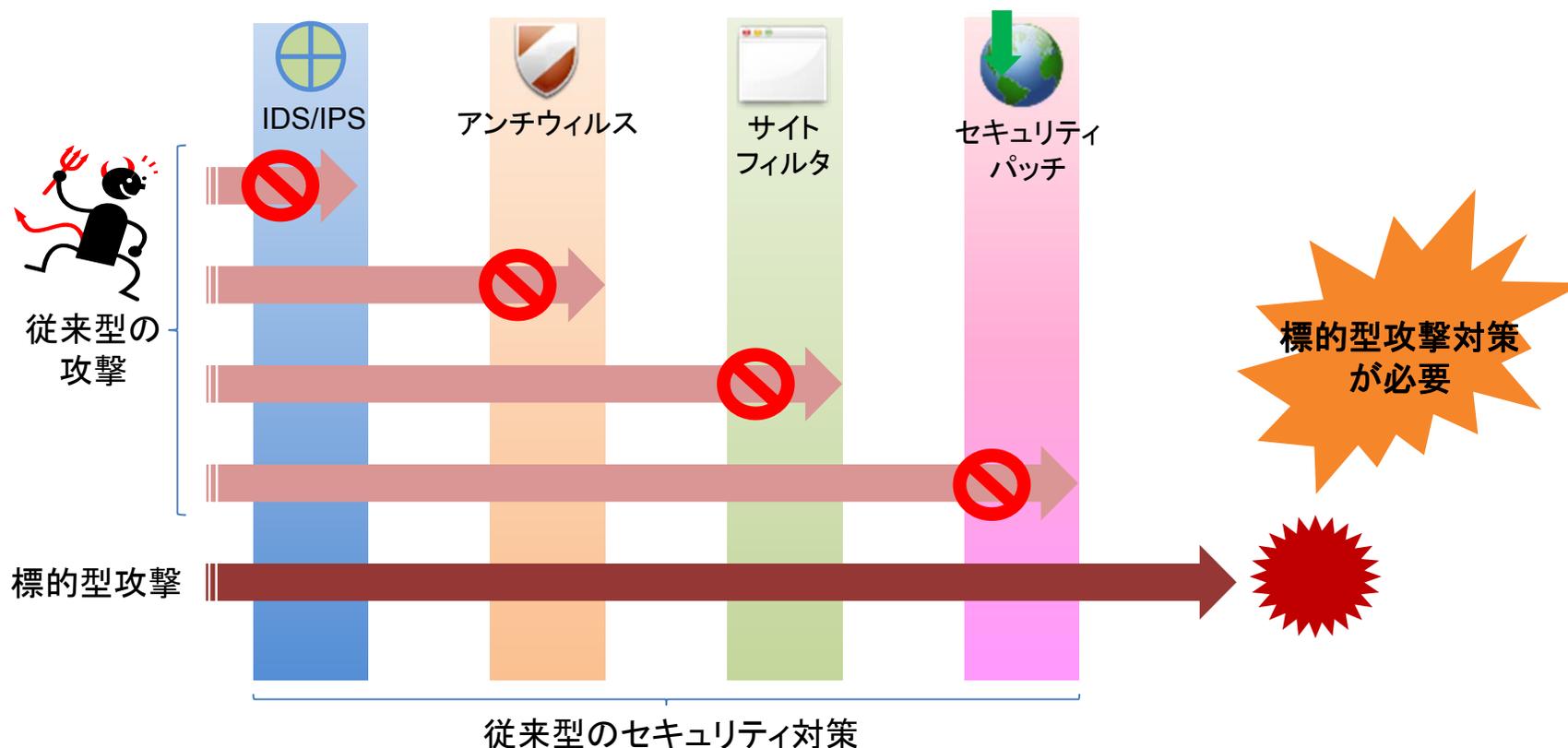
コーポレートマークには「1440」の文字と
スノーボードの回転をイメージした矢印で
設立当初から変わらない

「未踏の分野への挑戦」を表現



事業環境

標的型攻撃は従来型セキュリティ対策だけでは守り切れない

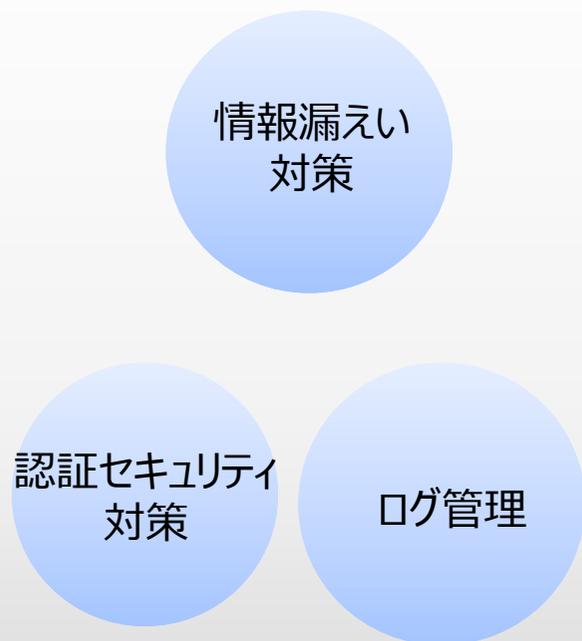


特定の組織団体に対して個別に作成される標的型攻撃マルウェアの場合、攻撃の事実が表面化しにくく、アンチウイルスベンダーの対応も遅れがち
標的型攻撃対策としては、従来のパターンファイルに依存せず、振る舞いで検知することが有効

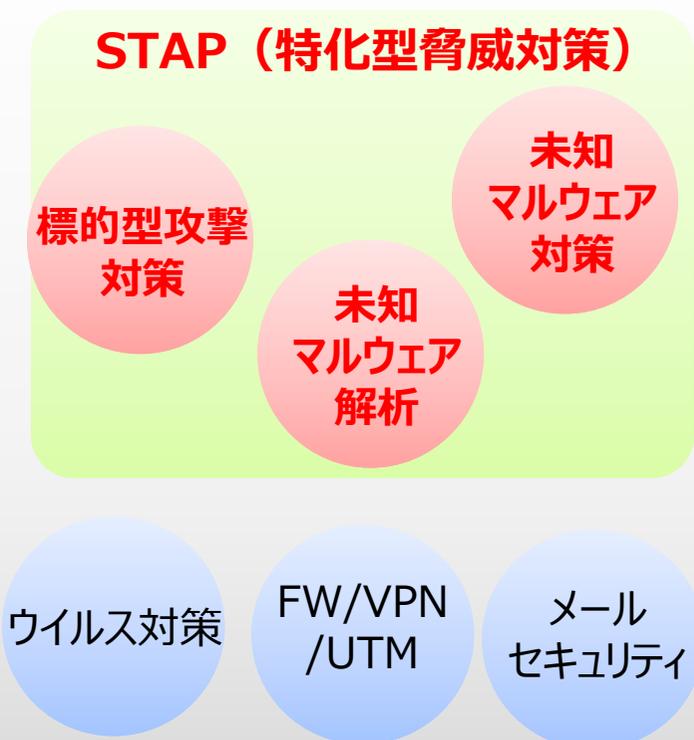
FFRIが注力する市場

情報セキュリティ市場

内部脅威対策



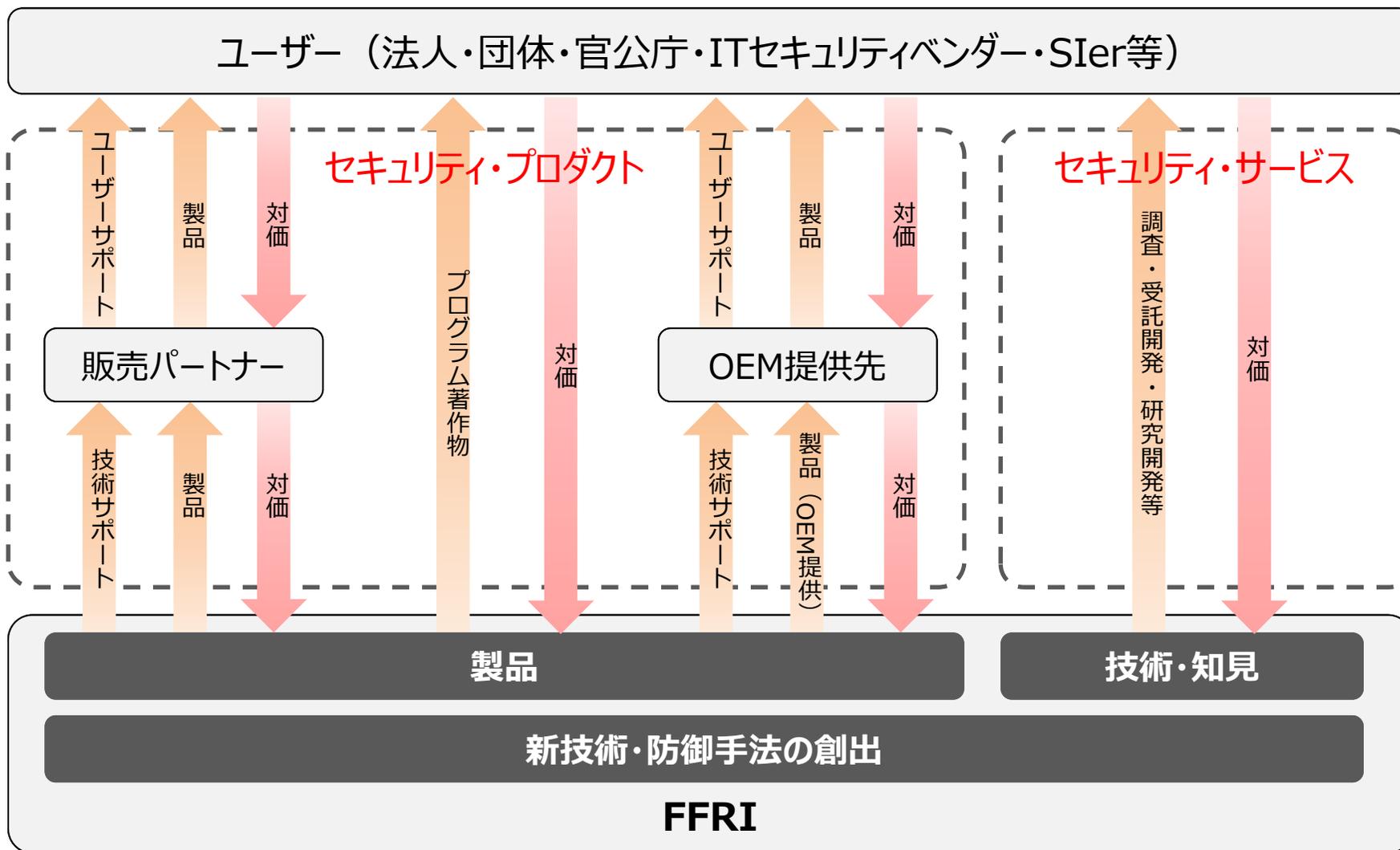
外部脅威対策





事業の内容・強み

事業モデル



主要なセキュリティ・プロダクト

名称	内容
FFR yarai	パターンファイルに依存しない、完全ヒューリスティック検知技術による標的型攻撃マルウェア対策製品で、未知・既知のマルウェア及びセキュリティ脆弱性を狙った攻撃を防御します。
FFR Raven	スマートフォンや情報家電、ネットワーク機器などネットワーク機能を持つ組み込み機器のセキュリティ堅牢性を検査するツールです。
FFR yarai analyzer	プログラムや文書ファイル、各種データファイルを自動的に解析し、マルウェア混入のリスク判定が可能なレポートを出力することで、自社内でマルウェア初動解析が可能です。
FFRI Limosa	インターネットバンキングにおけるMITB攻撃対策製品で、PCがMITBマルウェアに感染してもMITBマルウェアがブラウザに干渉できないような保護機構により攻撃から守ります。

セキュリティ・サービス

名称	内容
セキュリティ調査・分析・研究等	コンピュータ・システムのセキュリティ堅牢性調査と、実際にサイバー攻撃を受けた場合の影響調査などユーザーのニーズに応じたサービスを行います。
受託開発	顧客が運用しているネットワークシステムのセキュリティ強化を目的としたハードウェア・ソフトウェアへ、独自のサイバー・セキュリティ対策の仕組みを組み込む開発を請け負います。
標的型攻撃マルウェア検査サービス	機密情報漏洩のリスクを可視化し、対策検討含め、標的型攻撃に対する適切なリスク管理の実現を支援します。
Android端末セキュリティ分析サービス	Android端末における様々なセキュリティ上のリスクを分析し、対策に関する提言を行い、Android端末のセキュリティ脅威を分析します。
Prime Analysis	組織が抱える0-day脆弱性、標的型攻撃といった課題の解決を支援する包括的リサーチサービスです。
FFRI ExpertSeminar	セキュリティ技術者のための技術研修コースです。



FFRIの特徴

ヒューリスティック検知技術

国内での独自のR&D体制

技術力を裏付ける確かな実績

ヒューリスティック検知技術

ヒューリスティック	パターンマッチング
<p>マルウェア等の不正なプログラムを検知する際、パターンファイルによるマッチングではなく、マルウェア等がもつ特徴的なコードの構造や振る舞いを検知する手法です。</p> <p>これにより未知のウイルスによる攻撃を防御することができる他、攻撃者により標的に特化してカスタマイズされたマルウェアにも有効です。</p>	<p>パターンファイル（マルウェアが持つ特定の文字列や、特徴的な動作パターンなどが記録されているもの）と検査対象のファイルを照合することで、がマルウェアかどうか判定します。</p> <p>新しいマルウェアが出現するごとに対応するパターンファイルが必要であるため、新種や未知のマルウェアに対する防御機能はありません。</p>

パターンマッチング型アンチウイルスソフトと FFR yarai との違い



国内での独自のR&D体制



情報セキュリティに関するカンファレンスでの発表実績

- BlackHat、RSA Conference、CanSecWestなどセキュリティ業界で権威のある国際的な情報セキュリティカンファレンスで研究成果を多数発表。
- 弊社ホームページにて多数の研究成果を発表。



セキュリティ脆弱性発見に関する実績

100を超えるクリティカル脆弱性発見の実績有り

例：Microsoft Windows (LSASS脆弱性、wkssvc脆弱性、アニメーションカーソル脆弱性、GDI脆弱性、Office製品、Internet Explorer など多数)、Winny、一太郎、QuickTime、Realplayerなど他多数

記事、専門雑誌、新聞、NHKニュースなどメディアに多数掲載。

例：Windows標準搭載のIPv6スタックに脆弱性発見

報告日：2010年3月24日/公開日：2010年8月11日

※この脆弱性は独自検査ツール「FFR Raven」により発見



技術力を裏付ける確かな実績

- サイバーセキュリティに関する国家プロジェクトへの参画
 - 総務省の「官民連携による国民のマルウェア対策プロジェクトACTIVE」に参画
- サイバーセキュリティに関する国際的なプロジェクトへの参画
 - インターポールとNECのサイバーセキュリティ対策の提携に参画し、国際的なサイバー犯罪対策を強化するセキュリティソリューションの開発を支援
- 日本のサイバーセキュリティ人材育成の支援
 - セキュリティ・キャンプ等への講師派遣



INTERPOL Secretary General Ronald K. Noble氏（右）



「ACTIVE推進フォーラム第1回会合」 明治記念館(東京都港区)



成長戦略



成長戦略

1) 「FFR yarai」のデファクト・スタンダード化

2) 「法人・PC・国内」という基軸からの横展開

3) 新技術の研究開発

1) 「FFR yarai」のデファクト・スタンダード化

外部環境

標的型攻撃の
脅威が増大

未知脅威対策の
必要性の高まり



当社製品の特徴

ヒューリスティック
検知技術で
未知の脅威に
対抗



目指す姿

「FFR yarai」の導入が
PCのセキュリティ対策として
「デファクト・スタンダード」
となること

取組み

- 検知エンジンの強化
- 標的型攻撃の脅威と対策の啓蒙活動
- 営業体制強化

検知エンジンの強化

FFR yaraiに搭載する5つのヒューリスティックエンジン



標的型攻撃の脅威と対策の啓蒙活動

開催日	名称	テーマ
2014年4月	escar Asia 2014	組み込み機器のセキュリティとファジングによる対策
2014年5月	第11回情報セキュリティEXPO【春】	マルウェアの実態 ～バンキングマルウェア「Citadel」の解析から得られた近年のマルウェアの動向と対策～
2014年5月	CACS 2014	サイバーセキュリティの動向と未来予測
2014年6月	標的型攻撃 不正ログイン 巧妙化する脅威から身を守る術は	未知の脅威に対抗する！！～標的型攻撃に対抗するために「エンドポイント多層防御」の提案～
2014年7月	Factory 2014 Security & Network	基調講演「工場がネットワークにつながる時代に求められるセキュリティ」
2014年7月	標的型攻撃対策セミナー ～多層防御によるセキュリティ対策について～	「未知脅威対策」はお済みですか？ ～最新のサイバー攻撃に対抗するためには「未知脅威対策」が必須～
2014年7月	標的型攻撃時代のセキュリティ対策 第17回課題解決ソリューションセミナー	基調講演 サイバー脅威の変遷と 標的型攻撃への備え
2014年7月	Itpro ACTIVE製品選択支援セミナー 「標的型攻撃への対策～脅威への対策製品と製品選択のポイント」	未知の脅威に対抗する！！ ～標的型攻撃に対抗するために「エンドポイント多層防御」の提案～
2014年8月	ソフトウェア開発マネジメント交流会議	組み込み機器のセキュリティと ファジングによる対策



営業体制強化

目指すのはすべてのコンピュータ・システムへの当社製品導入

売上規模

従業員規模1,000人以上
官公庁、金融、情報通信、製薬、
重工業等
大手ITセキュリティベンダー及び
Sierの販売パートナーによる販売

従業員規模1,000人未満
流通系販売パートナーによる拡販
小ロット販売に耐える販売フロー及
びサポート体制の整備

Eコマース及び家電量販店等による
大量販売可能な体制整備
小ロット販売に耐える販売フロー及
びサポート体制の整備

コンシューマー

官公庁
大手企業

中規模
小規模法人

法人市場

現状、法人市場における
エンドポイント型の標的型攻撃
対策製品のシェアは独占状態で、
ホワイトスペースも大きい

現在

X年

X+α年

時期

2) 「法人・PC・国内」という基軸からの横展開

顧客

法人



個人

コンシューマーPC向け
FFR yaraiのリリース

デバイス

PC



スマート
デバイス

Androidモバイル端末向け
セキュリティソフトのリリース

市場

国内



海外

北米市場への拡販

コンシューマーPC向け FFR yarai

FFR yaraiの特徴・強み

- ✓ 5つのヒューリスティックエンジンにより既知・未知のマルウェアからPCを防御
- ✓ 頻繁なソフトウェアの更新が不要で動作が軽い

Android向け セキュリティ製品

投入製品の特徴

- ✓ アプリのユーザーの意図しない不正な動作をわかりやすく表示
- ✓ ヒューリスティック検知技術により悪意あるプログラムを検知
- ✓ 動作が軽いためバッテリー負担が少ない

3) 新技術の研究開発

将来顕在化する脅威に向けたシーズ型研究開発

- ✓ NFC技術のセキュリティ
- ✓ 車載ネットワークセキュリティの現状



次世代セキュリティ製品・サービス
提供のための技術蓄積

シーズ型研究開発からの実用化

- ✓ 2013/9
機械学習に基づくマルウェア判定技術の試作
- ✓ 2013/3
Android、Windows 7等のモバイルプラットフォーム
のセキュリティ機構に関する調査



2014/8
FFR yarai 2.5に機械学習
エンジン搭載



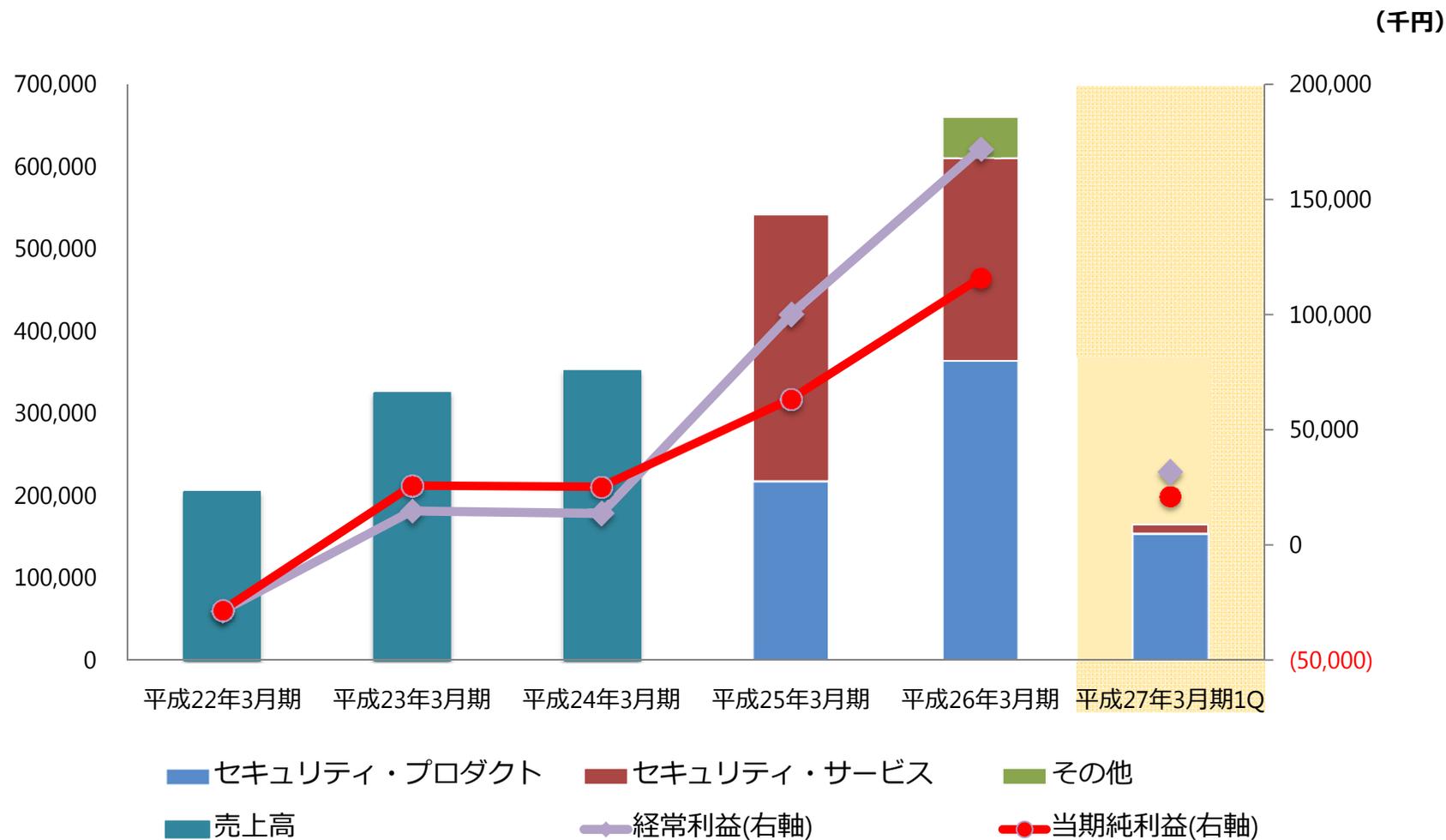
2014年（予定）
Android端末向け
セキュリティソフトのリリース



業績説明



業績の推移



業績サマリー (PL)

(単位：千円)

	平成22年 3月期	平成23年 3月期	平成24年 3月期	平成25年 3月期	平成26年 3月期	平成27年 3月期 1 Q
売上高 (千円)	204,518	324,660	351,318	541,777	660,250	164,778
経常利益 (千円)	△28,414	28,308	39,594	100,098	172,062	31,630
当期純利益 (千円)	△28,413	25,732	25,241	63,430	115,914	21,065
1株当たり純利益 (円) (注) 1.	△19.41	17.58	15.73	37.22	68.03	12.36

(注) 1.当社は平成26年6月11日付で株式1株につき300株の株式分割を行っております。
 そこで、平成22年3月期の期首に当該株式分割が行われたと仮定して算出した場合の1株当たり指標の推移を記載しています。
 2.平成22年3月期から平成24年3月期までの各数値については、監査法人による監査を受けておりません。

業績サマリー (BS)

(単位：千円)

科 目	平成25年 3月期	平成26年 3月期	平成27年 3月期 1Q	科 目	平成25年 3月期	平成26年 3月期	平成27年 3月期 1Q
流動 資産	476,407	822,240	919,690	流動 負債	153,695	248,884	306,091
				固定 負債	73,595	204,578	227,768
固定 資産	103,714	99,967	103,979	負債 合計	227,291	453,462	533,860
				純資産 合計	352,829	468,744	489,810
資産 合計	580,121	922,207	1,023,670	負債・ 純資産 合計	580,121	922,207	1,023,670

<本資料の取り扱いについて>

本資料に含まれる将来の見通しに関する記述等は、現時点における情報に基づき判断したものであり、マクロ経済動向及び市場環境や当社の関連する業界動向、その他内部・外部要因等により変動する可能性があります。

従いまして、実際の業績が本資料に記載されている将来の見通しに関する記述等と異なるリスクや不確実性がありますことを、予めご了承ください。